CRYPTOGRAPHIC METHODS AND APPARATUS USING WORD-WISE MONTGOMERY MULTIPLICATION

ABSTRACT

Cryptographic methods and apparatus are provided for determination of multiplicative inverses. A Montgomery radix is selected based on a wordsize, permitting word-wise Montgomery multiplication. Using word-wise Montgomery multiplication, methods and apparatus determine various multiplicative inverses with reduced computation time.